Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

~ Facebook Warns Targets ~ People Are Talking! ~ Firebee News Update!
~ NES Arrived 30 Yrs Ago ~ Ex-DEA Agent Gets Jail! ~ Windows 10 Update News!

~ No More Kid Pictures! ~ NSA's Cyber Concerns! ~ 11 Worst Web Scams!
~ Hackers Demand Ransom! ~ Google Fair Use Victory ~ USB Killer v2.0!

-* Halo Boss Has High Ambition! *-
-* Tech Firms Join Forces Against CISA *-
-* California Now Has Best Digital Privacy Law *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

Brrr! Our recent autumn weather has felt a little more like winter lately! While the weather folks tell us that our fall foliage has just about reached peak colors, my neighborhood still looks quite drab! It's been cold enough to get the colors going, but so far, the leaves have barely started to turn and they've not started to fall yet. I guess it will be an extended raking season this year!

Not much time to write some interesting comments this week even though there's a lot going on in the world lately. Busy at work, a few doctor appointments, and trying to catch up on some much-needed sleep has kept me busy. So, rather than take up much more of your valuable time, let's get to this week's issue!

Until next time...

=~=~=~=

FireBee News Update

by Fred Horvat

With the last submission to AONE about Web Browsing with the FireBee and the feedback I got on http://atari-forum.com it appears that something is not right with my FireBee Firmware or my FreeMiNT setup. With some followup messages on the forum it appears that the FireBee should be able to run the latest Test Builds of Netsurf 3.4. My FireBee cannot. I am going to reflash some of the FireBee Firmware and do a fresh install of the FireBee FreeMiNT 1.18 and test Netsurf 3.4 again. Hopefully this will correct any issues that I am having with the FireBee. I will then have to retest all the software that did not run on my FireBee to see if the software is compatible or not as now I am not sure. So hopefully in the next week I will be able to do this and report back my findings.

=~=~=~=

->In This Week's Gaming Section - Why Did Hideo Kojima Leave Konami?
"""""""""""""""""""""""""""""""""
Halo Boss Wants To Run Franchise Like George Lucas

The NES Arrived in America 30 Years Ago!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""

Why Did Hideo Kojima Leave Konami?

On Friday, October 9th, Hideo Kojima left the Tokyo offices of Konami, the video-game company where he had worked since 1986, for the last time. The departure ceremony, according to one of the hundred or so guests who attended, and who asked that I not use his name, took place at Kojima Productions, the director s in-house studio, and was a rather cheerful but also emotional goodbye. He said that he did not see Konami s president, Hideki Hayakawa, or its C.E.O., Sadaaki Kaneyoshi, at the party, but some of Kojima s colleagues from other studios showed up to pay their respects, as did many of the people who worked on his most recent directorial project, Metal Gear Solid V: The Phantom Pain. The game, which takes place in mid-nineteen-eighties Afghanistan and Zaire, made a hundred and seventy-nine million dollars on its launch day, in September more than the two highest-grossing films of the year so far (Avengers: Age of Ultron and Jurassic World) combined. In the past several decades, Kojima s name has become synonymous with such blockbusters, and with the Konami brand itself. His impending resignation had been rumored as early as March, but the fact of it remains startling as much as if Shigeru Miyamoto, the originator of Donkey Kong and the Mario brothers, left Nintendo.

Why would Konami drop its star game maker and shut down his studio? Although work on Phantom Pain is known to have been slower and more expensive than the company planned a Nikkei report estimated the cost of development at more than eighty million dollars Kojima s instinct to hold off the game s release until he was satisfied with its quality seems, by both critical and commercial standards, sound. As such, some people within the video-game industry contend that his resignation was less a result of personal or artistic differences than of tectonic changes in the business namely, the move away from console games and toward the domain of the mobile device.

That shift began in 2007, prior to the launch of the iPhone, when

the Japanese company GREE began to experiment with a new model for its online games. It started offering its products as free downloads to consumers, who then paid money for bonus content such as new characters, costumes, and levels. According to Serkan Toto, who runs the Tokyo-based consultancy Kantan Games, the so-called free-to-play model gained in popularity after the collapse of Lehman Brothers, in 2008, when the cost of television advertising in Japan plummeted. Companies mass-bought TV spots, contrasting their free games with the comparable expense of buying dedicated video-game systems and packaged software, he told me.

The tactic worked. Today, DeNA and GREE, the two largest mobile-game operators, count more than fifty million registered users between them. And although mobile games are cheap to produce, they can bring significant returns. A financial report from Mixi, the company behind Japan s current top mobile game, Monster Strike, suggests that the company is expected to make around one and a half billion dollars per year from this single title in Japan alone. Likewise, Konami s first mobile hit, Dragon Collection, helped boost its profits by almost eighty per cent between 2011 and 2012. As Jordan Amaro, a designer who worked with Kojima on Phantom Pain, put it, Why risk producing pricey and sophisticated games in an age that favors indulgence in shallow, convenient entertainment? Ryan Payton, who worked at Konami between 2005 and 2008, went even further. We ve seen the end of the console-game market in Japan, he said. Even by the time Metal Gear Solid IV shipped, in 2008, I felt like our team was one of just a handful of Japan-based developers who were still fighting to produce blockbuster games.

Although the mobile-game market may be irresistible to profit-chasing executives, Kojima and other ambitious directors like him have seemed unwilling to squeeze their creative vision into the snug confines of a phone or tablet screen. (Kojima declined to speak with me for the time being, citing a legally binding agreement with his former employer, but when I interviewed him in 2012 he said that his childhood love of cinema has had a profound effect on his art.) There have sometimes been penalties for those who fail to adapt to the changing industry. According to Kotaku s partial translation of the original Nikkei article, such employees have, in the past, been redeployed to the assembly line at Konami s pachinko factory or ordered to work as security guards or janitors at the company s fitness clubs. (Konami did not immediately respond to requests for comment on this and other claims.) Tak Fujii, a former senior producer at Konami, who left the company in 2014 because of ill health, sees no issue with this kind of radical reorganization. I saw many colleagues unwillingly reassigned, he said. Most of them blamed everyone but themselves. But they were not willing to adapt. They were waiting for the golden days to return. All they had left were legendary stories of their products, which are no longer relevant for either the technology or the market.

Hayakawa, who became president of Konami in April, acknowledged in an interview with Nikkei in May that mobile is where the future of gaming lies. The company claims that it is not abandoning console games entirely; as the sales of Phantom Pain attest, big-budget projects can still be profitable. Nevertheless, the effect of the closure of Kojima Productions on other game makers has been significant. It s a rare case of a highly successful

studio being closed down, so obviously everyone is in a state of shock about it, I think, Hajime Tabata, the director of Final Fantasy XV, a console game that, like Metal Gear Solid, has been in development for years, at vast cost, told me. But we believe that we can survive. At least, until the company decides to close us down. The decline of major console games has been mirrored in smaller, less well-known titles, too. The Japanese games with which most players are familiar have always been the outliers, David McCarthy, of the Tokyo-based developer Cybird, told me. But there has always been a huge iceberg of titles beneath the surface that Western gamers rarely glimpse. The growing cost of console development, allied to a shrinking domestic market, have made these games increasingly unviable without international success.

It s likely that, after Kojima s non-compete clause expires, in December, he will find a new studio and continue making lavishly produced games. But these future projects will be anomalies in a mobile-dominated Japanese market. Although Western fans may mourn the loss, McCarthy doesn t share their despondency. Honestly, I am not so sure that any threat to yet another shouting, shooting game full of American grunts saving democracy from the wiles of dark-skinned terrorists is any great loss to the art, he said.

Halo Boss Wants To Run Franchise Like George Lucas Did With Star Wars

Bonnie Ross, head of Halo developer 343 Industries, has revealed some interesting new insight into Microsoft’s blockbuster sci-fi shooter series. It might surprise you to learn that when she helped create 343 Industries in 2009, not everyone inside Microsoft thought Halo would be around much longer.

"People felt like, ’Let’s get another Halo or two out, and it’s the end of the franchise,’" Ross recalled in a new interview with Bloomberg Business.

When discussing the future of the Halo series and what she wanted to do as 343’s general manager, Ross said she asked to be granted George Lucas-like control over the franchise. Lucas created the Star Wars franchise and oversaw it until he eventually sold the series to Disney in 2012 for $4.05 billion.

"The thing I asked for was: If I take it over, I want to be George Lucas," she said. "I want to own everything, and I want to do things differently."

Though there might have been some initial internal skepticism about the long-term appeal of the Halo brand, that no longer seems to be the case. In a previous interview, Ross said Microsoft’s hope is for the Halo franchise to remain popular for at least another 30 years.

Halo franchise director Frank O’Connor is also featured in Bloomberg’s story. He was working at Bungie at the time, and was part of the team that oversaw Bungie’s handover of the Halo series to Microsoft. He says he remembers meeting with Ross and expecting her to be a "suit" focused on business above all else.

"Bonnie came in and really surprised everyone," he said. "Because she'd read all the novels, she was deeply immersed in the fiction, and she'd played all the games."

O'Connor later quit Bungie and joined Ross at 343 Industries.

The next release from 343 is Halo 5: Guardians, which launches on October 27 for Xbox One. For lots more on the Halo franchise and the formation of 343, be sure to read the full Bloomberg story.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!

The NES Arrived in America 30 Years Ago

The original NES.

Nintendo's Famicom console may have celebrated its 30th birthday back in July of 2013, but it was 30 years ago this week that the Nintendo Entertainment System technically made its debut.

On October 18, 1985, Nintendo renamed the Famicom and released it in North America as the NES. Not only did it ensure Nintendo would have a future outside of Japan, but it ensured gamers would have a future playing games at home.

At the time, gamers were still feeling the aftershocks of the 1983 home console crash. Scared off by falling stocks and an abundance of low-quality titles, most retailers at the time suspected home video games were nothing more than a fad and backed away. The glory days of the Atari 2600 and Intellivision came to a stunningly fast end.

Nintendo faced an uphill battle getting the NES on store shelves. The company first showed off the system at the Consumer Electronics Show in June of 1985, and it quickly ran into skepticism. Retailers, still jaded, were afraid of its complexity and balked at the thought of promoting another video game console.

The reception convinced Nintendo to delay the launch. The company smartly made some changes, including putting games onto distinctive looking cartridges. It also packaged an accessory called R.O.B. (Robotic Operating Buddy), a small robotic toy that worked with two games and was meant to make the NES look more sophisticated than past consoles.

Finally, on October 18, Nintendo released the console in limited quantities in New York. Only about 50,000 units were sold through the holidays, but it was enogh to prove to Nintendo (and

retailers) that the system had a future. In early 1986, the system was made available in other cities.

Ultimately, it was the NES s incredible lineup that helped the system find its footing. Launching with 17 games, the NES enjoyed a terrifiic suite of games, including Duck Hunt, Excitebike, Hogan’s Alley, and, of course, Super Mario Bros. Gamers in short order remembered why they had embraced the hobby in the first place, and the path was set for the industry’s revival.

By the time the console was discontinued in 1995, over 700 NES games had been released and over 30 million systems had been sold in America alone. And the rest, as they say, is history. Happy 30th, NES!

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Google, Facebook, Amazon et al Join Forces Against Incoming Cybersecurity Law

Some of the world’s largest tech firms have come together to issue a public protest against a controversial US cybersecurity bill.

The Cybersecurity Information Sharing Act (CISA), due to be laid out for Senate consideration in the next few weeks, has noble aims based around the sharing of threat intelligence between private companies and the government.

But its critics say it does not adequately protect users’ privacy. One of those, the Computer & Communications Industry Association (CCIA), says the current proposal fails to "limit the permissible uses of information shared with the government."

Furthermore, the association says the existing bill will allow network defensive measures that could inadvertently cause harm to innocent third parties.

In an open letter published Thursday, the CCIA, which represents Google, Facebook, Microsoft, Amazon, and eBay, as well as several other major tech firms, said it approved of the goal of the legislation - to aid in the fight against crime and terrorism - but could not support it in its current form, saying it:

...recognizes the goal of seeking to develop a more robust system through which the government and private sector can readily share data about emerging threats. But such a system should not come at the expense of users’ privacy, need not be used for purposes unrelated to cybersecurity, and must not enable

activities that might actively destabilize the infrastructure the bill aims to protect.

The CCIA says it is keen to work with the US government to improve CISA, as well as other cybersecurity legislation, but it hopes the end result will be based more around a voluntary framework backed up by a strong level of privacy protection and with appropriate restrictions on use baked in.

The current bill has attracted wide support from both Democrats and Republicans, but there are some dissenting voices on both sides of the political spectrum:

Democrat Ron Wyden of Oregon said:

> CCIA represents some of the biggest names in tech and their opposition to the current version of Cisa is a shot in the arm for those of us fighting for privacy and security...
>
> These companies understand it is untenable and bad for business to enact flawed 'cybersecurity' policies that infringe on users' privacy while doing little to prevent sophisticated hacks. By coming out against this bill, CCIA's members, including Google, Yahoo, and Facebook, have made the clear statement that they have their users' backs.

Republican Rand Paul has been less bashful in expressing his distaste for CISA - a rewrite of the highly controversial Cyber Intelligence Sharing and Protection Act (CISPA) - saying that it would "transform websites into government spies" by granting:

> new spying powers that gut privacy laws and allow internet providers and websites to hand over personal data to ANY agency in the federal government.

Furthermore, Rand says, CISA would trample Fourth Amendment privacy protections, circumvent the Freedom of Information Act and give government agencies the ability to access citizens' private information without a warrant, all without actually improving the government's ability to prevent cyber attacks.

Not all government agencies are overly enamoured by the new bill either - in August, Department of Homeland Security Deputy Secretary Alejandro Mayorkas, said the Act "raises privacy and civil liberties concerns", and the legal immunity given to data-sharing companies could "sweep away important privacy protections."

Proponents of the bill - such as Senate Intelligence Committee Chairman Richard Burr and Vice Chairman Dianne Feinstein - have an entirely different point of view of course, emphasising how the sharing of information is entirely voluntary, yet eminently essential.

The pair cited the recent T-Mobile/Experian breach, although there's no evidence it could have been prevented had there have been better lines of communication between industry and government.

California Now Has the Nation s Best Digital Privacy Law

California continued its long-standing tradition for forward-thinking privacy laws today when Governor Jerry Brown signed a sweeping law protecting digital privacy rights.

The landmark Electronic Communications Privacy Act bars any state law enforcement agency or other investigative entity from compelling a business to turn over any metadata or digital communications including emails, texts, documents stored in the cloud without a warrant. It also requires a warrant to track the location of electronic devices like mobile phones, or to search them.

The legislation, which easily passed the Legislature last month, is the most comprehensive in the country, says the ACLU.

This is a landmark win for digital privacy and all Californians, Nicole Ozer, technology and civil liberties policy director at the ACLU of California, said in a statment. We hope this is a model for the rest of the nation in protecting our digital privacy rights.

Five other states have warrant protection for content, and nine others have warrant protection for GPS location tracking. But California is the first to enact a comprehensive law protecting location data, content, metadata and device searches, Ozer told WIRED.

This is really a comprehensive update for the modern digital age, she said.

State senators Mark Leno (D-San Francisco) and Joel Anderson (R-Alpine) wrote the legislation earlier this year to give digital data the same kinds of protection that non-digital communications have.

For what logical reason should a handwritten letter stored in a desk drawer enjoy more protection from warrantless government surveillance than an email sent to a colleague or a text message to a loved one? Leno said earlier this year. This is nonsensical and violates the right to liberty and privacy that every Californian expects under the constitution.

The bill enjoyed widespread support among civil libertarians like the American Civil Liberties Union and the Electronic Frontier Foundation as well as tech companies like Apple, Google, Facebook, Dropbox, LinkedIn, and Twitter, which have headquarters in California. It also had huge bipartisan support among state lawmakers.

For too long, California s digital privacy laws have been stuck in the Dark Ages, leaving our personal emails, text messages, photos and smartphones increasingly vulnerable to warrantless searches, Leno said in a statement today. That ends today with the Governor s signature of CalECPA, a carefully crafted law that protects personal information of all Californians. The bill also ensures that law enforcement officials have the tools they need

to continue to fight crime in the digital age.

The law applies only to California law enforcement entities; law enforcement agencies in other states would be compelled by the laws in their jurisdictions, which is why Ozer and others say it s important to get similar comprehensive laws passed elsewhere.

The law places California not only at the forefront of protecting digital privacy among states, it outpaces even the federal government, where such efforts have stalled.

Civil libertarians and others have long lobbied federal lawmakers to update the Electronic Communications Privacy Act to offer such protection nationwide. An amendment to that law has been wending through Capitol Hill, where it has 300 co-sponsors. But the proposal is less comprehensive than the law Brown signed, and would merely focus on digital content. Currently, the federal ECPA requires a warrant for stored content that is newer than 180 days; the amendment would extend the warrant requirement to all digital content regardless of age.

California has long led the way in privacy protection. Voters amended the state constitution in the 1970s to provide explicit privacy rights far more robust than those guaranteed by the Fourth Amendment of the US Constitution. But while the state amendment ensured a right to privacy for all Californians, lawmakers couldn t envision the technological advances that would come in the decades to follow. The law that Brown signed today closes surveillance loopholes left by that amendment and codifies what was intended by that privacy right, Ozer says.

We certainly hope that this bill is a clarion call [for the federal amendment], she told WIRED. This is not only a comprehensive update for all Californians, but hopefully is a model for making sure that all Americans have this kind of digital privacy protection.

California Nixes Warrantless Search of Digital Data

In what’s being called a landmark victory for digital privacy, California police will no longer be able to get their hands on user data without first getting a warrant from a judge.

Governor Jerry Brown on Thursday signed the California Electronic Communications Privacy Act (CalECPA), SB 178, which requires state law enforcement to get a warrant before they can access electronic information about who we are, where we go, who we know, and what we do.

US privacy rights groups have long been concerned that law enforcement hasn’t considered it necessary to get a search warrant before they can search messages, email, photos and other digital data stored on mobile phones or company servers.

States such as California, tired of waiting around for Congress to update 29-year-old federal electronic privacy statutes, are

taking reform into their own hands.

The American Civil Liberties Union (ACLU) called CalECPA a "landmark win".

Nicole Ozer, Technology & Civil Liberties Policy Director at the ACLU of California:

> This is a landmark win for digital privacy and all Californians. We hope this is a model for the rest of the nation in protecting our digital privacy rights.

Hanni Fakhoury, senior staff attorney for the Electronic Frontier Foundation, told NBC News that while California isn't the first state to guarantee protections such as these - Utah and Maine have similar laws on the books - the nation's most populous state has passed the most protective law to date.

The bill was sponsored by Democratic Senator Mark Leno and Republican Senator Joel Anderson.

The ACLU published an article by the two senators in which they had decried the state's antiquated privacy laws:

> Technology has advanced exponentially, but California s privacy laws are still stuck in the digital dark ages. Law enforcement is increasingly taking advantage of outdated privacy laws to turn mobile phones into tracking devices and access sensitive emails, digital documents, and text messages without proper judicial oversight.

As it is, 82% of Californians have voiced support for the end to warrantless digital information searches.

According to the ACLU, CalECPA is a direct response to an "exponential growth in law enforcement demands for digital information" that's seen demands to Google nearly triple over the last five years.

Twitter, meanwhile, has reported a 52% jump just this past year.

In its own transparency report, Twitter revealed that it received 4,363 government data requests in the first half of 2015, around half of which were in the US.

Twitter complied with the US requests 80% of the time.

According to the senators who authored the bill, AT&T received more than 64,000 demands for location information in 2014; Verizon received more than 15,000 demands for location data in the first half of 2014, and only one-third of those came with a warrant.

According to Senator Leno, that situation ended on Thursday:

> That ends today with the Governor s signature of CalECPA, a carefully crafted law that protects personal information of all Californians. The bill also ensures that law enforcement officials have the tools they need to continue to fight crime in the digital age.

The tools to keep fighting crime to which Senator Leno referred include a number of exceptions: if police or another government entity believe that a device has been lost or stolen, they can access information on the device in order to identify, verify or contact its owner.

What's more, an emergency provision allows a government entity to search a device if it believes that "an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information."

That doesn't completely let the government off the hook, though - the agency doing the search will have three days from obtaining data in which it will still have to file for a warrant.

Facebook Will Notify You If The Government Hacks Your Account

Facebook has launched a new feature that notifies users if their accounts have been targeted by government-sponsored hackers.

In a one billion-plus users about how to secure their accounts Facebook's chief security officer, Alex Stamos said users would be notified "if we believe your account has been targeted or compromised by an attacker suspected of working on behalf of a nation-state."

The notification will advise users to turn on a feature called Login Approvals, which sends them a new security code that must be inputted each time an account is accessed from a new device or browser.

Stamos said that receiving such a notification was not an indication that Facebook's central systems had been compromised but rather that the user's computer or mobile may be infected with malware and should be rebuilt or replaced if possible.

Facebook would not reveal how it attributed certain attacks to state-sponsored actors, Stamos added, but that it would only use the notification system "where the evidence strongly supports our conclusion."

In 2013, conducting widespread surveillance operations, including the allegation that the U.S. National Security Agency hacked directly into the servers of nine internet firms including Facebook.

North Korea was also accused of state-sponsored hacking after the December 2014 cyberattack on Sony Pictures Entertainment, which resulted in the personal details of around 6,000 Sony employees being leaked online, as well as information about upcoming films and salaries of the company's top executives. North Korea denied any involvement.

During his recent visit to the U.S., Chinese President Xi Jinping denied that Beijing engages in state-sponsored hacking.

Facebook To Warn You of Targeted Attacks - Check This Security Setting Anyway

Facebook has announced that it will notify users it suspects are being targeted by nation states and urge them to take extra security precautions.

Alex Stamos, Facebook's chief security officer, explained the new notifications in a 16 October blog post, saying users will only receive the warnings if Facebook has strong evidence suggesting they are being targeted by nation-state sponsored attackers.

If the social network believes you are under attack from state-sponsored hackers, it will show a pop-up message in your feed explaining that you may have been targeted.

The message asks, but does not require, those users to turn on an extra layer of protection for their account called Login Approvals.

Stamos said Facebook "will have always taken steps to secure accounts that we believe to have been compromised," but will show the warning to users because these attacks may be "more advanced and dangerous" than others.

This is how the message looks in the desktop version of Facebook:

Facebook notification

Jay, we believe your Facebook account and other online accounts may be the target of attacks from state-sponsored actors. Turning on Login Approvals will help keep others from logging into your Facebook account. Whenever your account is accessed from a new device or browser, we'll send a security code to your phone so that only you can log in. We recommend you also take steps to secure the accounts you use on other services.

Because of the persistence of state-sponsored attackers, anyone whose Facebook account is under attack by a nation state is probably also being targeted on other services, so Facebook encourages securing those accounts as well.

Google began sending similar warnings to Gmail users back in 2012.

Just like Google, Facebook says it can't reveal how or why it suspects state-sponsored attacks, for fear of giving away useful information to attackers about security methods.

Nation states may target individuals for political or national security reasons, but also attack individuals to gain access to their employers' intellectual property or customer data, for example.

Countries like North Korea and China have been suspected of sponsoring attacks on private companies.

Hackers affiliated with the Chinese military were indicted by the

US two years ago for allegedly hacking into several US steel companies.

The US claims the Chinese hackers used phishing emails and malware to gain access to email accounts of company officials, in order to steal information that would benefit Chinese state-run steel companies in trade disputes.

Targeted or not, extra security is always a good idea

Even if nation states aren't likely to target you personally, it would be a shame to fall into the trap of thinking "no one's interested in little old me."

As Naked Security expert Paul Ducklin pointed out in a post describing all the bad excuses we make for neglecting our security, we are all on cybercriminals' radars:

> We're all in the sights of cybercrooks somewhere, and we owe it to ourselves and to everyone else to do the best we can to thwart them.

Today's cybercriminals are typically in the business of making money, and to do that they want to compromise as many users and devices as possible.

One method for attackers to gain access to your accounts is to implant malware on your computer that can steal passwords.

Malware of this sort can get on your computer in various ways, such as through boobytrapped email attachments, or by visiting a malicious website harboring malware that downloads automatically (called a drive-by download).

Malware can also spread via Facebook.

We recently learned of a hacker using a type of malware called a "Facebook Spreader" to compromise Facebook accounts via malicious links in Facebook chat messages.

In August, a US-based hacker named Eric Crocker pleaded guilty to spreading Facebook malware to hijack thousands of accounts in order to send spam.

Just like Facebook recommends, we think it's a good idea to add extra layers of security to your accounts, such as login verification or two-factor authentication.

Even if you're not likely to be a target of a nation state, that's no reason to become easy prey for common cybercriminals.

How to turn on Facebook Login Approvals

When you turn on Facebook Login Approvals, you'll need to enter a special one-time code whenever you log into Facebook from an unrecognized device or browser.

You'll receive the codes on your phone as a text message, so Facebook needs your mobile phone number to send Login Approval alerts.

Login Approvals are similar but more secure than Login

Notification, which alerts you when your account is accessed from a new device or browser, but without requiring a code.

To turn on Login Approvals:

Click the down arrow at the top right of any Facebook page
Go to Settings > Security
Click on Login Approvals
Check the box and click Save Changes

Finally, once you've set that up, make sure you change this setting so you can't be searched for by phone number.

NSA Chief: These Are The 3 Cyber Threats That Keep Me Up at Night

Admiral Michael Rogers, director of the National Security Agency and US cyber commander, doesn t think that the United States will ever have a digital equivalent of Pearl Harbor.

Speaking on stage at the Wall Street Journal s WSJDLive conference, Rogers dismissed that analogy because he doesn t think that a massive cyber attacks could ever be as surprising today as the attack on Pearl Harbor was in 1941.

It s not a matter of if, it s a matter of when.

Rogers outlined three things that concern him the most when thinking about cyber-threats to the United States:

1. Cyber attacks that do infrastructure damage

 It is only a matter of when that someone users cyber as a tool to do damage to the critical infrastructure of our nation, Rogers said.

 I m watching nation states, groups within some of that infrastructure. At the moment, it seems to be really focused on reconnaissance and attempting to understand the characteristics of the structure, but it s only a matter of time I believe until someone actually does something destructive.

2. Data manipulation

 Historically, we ve largely been focused on stopping the extraction of data and insights, whether for intellectual property for commercial or criminal advantage, but what happens when suddenly our data is manipulated and you no longer can believe what you re physically seeing? he said.

 As a military guy, who s used to the idea that, I can look at a display, I can look at a set of data, and I can very quickly draw conclusions and start to make risk-based decisions quickly, what happens if that gets called into question? I believe that s going to happen.

3. Non-state actors

What happens when a non-state actor, who literally has no interest in the status quo take ISIL for an example, whose vision of the world is diametrically opposed to ours starts viewing the web as not just a vehicle to generate revenue, to recruit, to spread the ideology, but instead they view it as a weapon system? he asked hypothetically on stage.
This stuff is going to happen

Rogers says that he believes that all these concerns will actually play out.

I fully expect that during my time as the commander and the director of the NSA, this stuff is going to happen, he said. And the nation is fully counting on us to be ready.

The NSA has faced intense scrutiny since former National Security Agency contractor Edward Snowden leaked documents revealing many of its intelligence apparatus, including global surveillance tactics.

Hackers Demand Ransom from British Telecom TalkTalk

British telecom TalkTalk said it has received a ransom demand following a "significant and sustained cyberattack" that put the data of four million customers at risk.

"We were contacted by someone claiming to be responsible, and seeking payment," the company said.

TalkTalk is one of Britain’s leading phone providers. It has admitted that its website was hacked earlier this week, and that information including the date of birth, address, credit card, and bank details of its four million customers might have been stolen.

Police have launched a criminal investigation, but no arrests have been made. The scale of the breach is still being investigated, police said.

"We take any threat to the security of our customers’ data extremely seriously and we are taking all the necessary steps to understand what has happened here," TalkTalk CEO Dido Harding said in a statement.

TalkTalk said it noticed unusual activity on its website on Wednesday, and took the site offline in an effort to protect data. The company said the initial attack was later found to be a DDOS denial of service attack.

It admitted not all data were encrypted, but said its systems were "as secure as they could be."

"Unfortunately these criminals are very smart and their attacks are becoming ever more sophisticated," the company said in a statement.

TalkTalk’s shares in London were down as much as 10 percent after

the attack came to light Friday morning (October 23).

Google’s Fair Use Victory Is a Win for Us All

Something crazy happened Friday in the weird world of intellectual-property law. A judge said it was okay to copy all of a copyrighted work and then share bits of it with the public even if you re a giant tech company and then explained clearly how that makes sense and makes us better off.

That makes Friday s Google Books ruling from the United States Court of Appeals for the Second Circuit not just good for Google, but good for readers everywhere. We all benefit when the author of a book or a movie or a record or another creative work doesn t get to veto every possible reuse and remix of it.

This case turned on Google s project, announced in 2004, to scan and index the full text of millions of books (lent to it by libraries) so that readers could search their contents and see brief snippets of matching text.

The Authors Guild, an association of American writes that dates to 1912, sued Google in 2005 for infringing its members copyrights and damaging the market for their work. Ten years later during which a proposed $125 million settlement between Google and the Guild was scuttled by a judge a unanimous three-judge Second Circuit panel found Google was within its fair-use rights to run this project.

Judge Pierre Leval s 48-page ruling focuses on the often overlooked first principle of intellectual property in U.S. law. As he wrote: The ultimate goal of copyright is to expand public knowledge and understanding. Improving the ability of creators to make a living through copyright is a pleasant side effect, not the fundamental point of the exercise.

But how do you get from there to granting Google permission to copy all of a book? Through Section 107 of the Copyright Act, which allows for fair use exceptions to copyright without actually defining what that phrase should mean in practice.

Judge Leval applied that section s somewhat vague criteria to the Authors Guild s claims and found them wanting every time. Google copied entire books? That transformed them into a new searchable medium that allows things like Ngram queries for the popularity of certain words over time. Google s a profitable company? Not a deal-breaker, since such fair-use exercises as news reports and book reviews are all normally done commercially for profit.

Most important, what about Google Books effect on the market for, you know, books? There s none worth fighting over, Leval held: A Google Books snippet may help you check a fact, but you can t claim copyright over a data point like that.

But courts haven t always had such a forgiving view; their sense of fair use has shifted considerably since the 1984 Supreme Court case in which the Betamax VCR was almost held illegal.

This is why people argue over fair use all the time: Not only do the lawyers involve not agree, they sometimes don t even agree with themselves.

For example, Berkeley law professor Pamela Samuelson and University of Maryland law professor James Grimmelmann separately said that under the pre-search-engine definition of fair use what Samuelson called a conventional role of fair use Google Books would flunk that test.

As Grimmelmann wrote, the scanning and indexing that Google does not just to books but to Web pages was once seriously contested and now is not. It took multiple cases to conclude that it s okay for a search engine to copy and index somebody else s Web page, then show a preview of that to visitors.

Consider another case that involved a for-profit company duplicating copyrighted material, but in a way that hardly threatened to steal a sale from a copyright holder: MP3.com, the site that in 2000 lost a court case over a feature that let listeners upload the track lists from their CDs, then listen to MP3.com s copies of those songs and only those songs over the Internet.

Grimmelmann called that probably no longer good law. By 2011, Amazon had no qualms over launching its Cloud Player, a service functionally identical to MP3.com s offering, without getting permission from every record label.

Both law professors are strong fair-use advocates, yet neither was willing to call another widely criticized copyright case   this year s jury verdict that Pharrell Williams, Robin Thicke and T.I. s Blurred Lines infringed Marvin Gaye s Got to Give It Up   an unreasonable ruling. See, it s complicated!

One thing that hasn t changed much during this expansion of fair use is the willingness of copyright holders to indulge in transparent control-freakery. Sometimes, they still get away with it.

See, for instance, the NFL s absurd complaint that posting GIFs of plays threatens the market for watching football games, which Twitter took seriously enough to suspend two accounts. See also, last year s ruling that invented an entirely new category of software copyright.

(At least U.S. copyright holders have yet to imitate some of the crazier ideas afloat in the E.U., like requiring search engines to pay a royalty for displaying a snippet of news stories or restricting the commercial use of photos or videos taken from public spaces of buildings and sculptures.)

Another thing that hasn t changed: Copyfight" litigation is not a good proposition for startups short on cash and time. You may not like the size and reach of a Google, but when it invests some of its resources in fair-use fights, the benefits aren t confined to its corporate campus.

USB Killer v2.0 Latest USB Device that Can Easily Burn Your Computer

In March, a Russian security researcher devised a weird USB stick that is capable of destroying sensitive components of a computer when plugged-in.

Now, the same researcher, nicknamed Dark Purple, has launched a new version of his computer-frying USB Killer pendrive USB Killer version 2.0.

USB Killer 2.0 is much more powerful than the previous version and is able to "kill" more than just a PC it is plugged in.

The first version of USB Killer was consist of a DC/DC converter, a few caps and an FET. When plugged into a system, the converter in the USB Killer would charge the caps up to -110V, apply that voltage to signal lines of the USB interface, and repeat the entire process until everything possible in the computer is broken down.

However, the second version of USB Killer dump -220V directly onto the signal lines of the USB interface, which is powerful enough to damage practically any computer with a USB port.

Another major improvement in the new version of USB Killer is the reaction rate. Once plugged into a computer, USB Killer 2.0 takes only a few seconds for the PC to shut down and stop working.

While testing his USB Killer 2.0 stick, Dark Purple destroyed his brand new Lenovo Thinkpad X60 laptop. You can watch the video demonstration given above that shows the attack in work.

"Do not worry about the laptop, the new motherboard is on the way - and the laptop will live again," Dark Purple wrote in a blog post. "Originally did not plan to restore it, the laptop was purchased specifically for the test."

Killer USB is not at all a new concept, USB drives are used as a valid weapon to compromise the system in air-gapped networks.

Stuxnet worm is one of the real examples that was designed to destroy centrifuges at the Nuclear facility, and all this started with a USB drive.

So it’s not false to say that a computer could be converted into a bomb because a hacker can probably make your computer explode as well.

Therefore, next time if you find a USB stick that doesn’t belong to you, just beware before inserting it into your laptop. You could lose your Laptop, along with all your important files and data stored in it.

Corrupt Ex-DEA Agent Carl Force Gets 6 Years for Extorting Silk Road

A former federal agent who lined his pockets with bitcoins extorted from the black market site Silk Road has been sentenced to 78 months - more than 6 years - in prison.

Former Drug Enforcement Administration (DEA) agent Carl Force agreed, in June, to plead guilty to squeezing what was then valued at around $50,000 worth of Bitcoin (about £32,000) from Silk Road's creator, Ross "Dread Pirate Roberts" Ulbricht.

Force had posed as a drug dealer and convinced Ulbricht that he had information on a DEA investigation into the site.

Also in June, Ulbricht was sentenced to life in prison without parole.

Force was one of legions of undercover agents that infiltrated Silk Road's user base. In its report on Ulbricht's sentencing, the FBI cited "more than 60 individual undercover purchases of controlled substances".

A couple of those agents were bad apples.

Instead of reporting the payment to the DEA, Force funneled the digital currency into his own personal accounts.

In late August, Secret Service agent and computer expert Shaun Bridges also pled guilty to charges of obstruction of justice and money laundering for using a Silk Road administrator account to steal around 20,000 bitcoins from various dealers.

At the time, that sum was valued at around $820,000 (about £530,000).

Bridges and Force worked together on the Silk Road investigation.

According to the criminal complaint, Force went under the user name "French Maid" to offer Ulbricht information for $98,000 (about £63,400) in bitcoin that he deposited into his own, personal accounts.

While prosecutors had pushed to sentence Force to 87 months in prison, his defence asked for a shorter sentence - 48 months - due to mental health issues and a family history of alcoholism and abuse.

Force apologized in court on Monday for a betrayal that the presiding judge called "breathtaking."

US District Judge Richard Seeborg had this to say:

> The extent and the scope of Mr. Force's betrayal of public trust is quite simply breathtaking. It is compounded by the fact that it appears to have been motivated by greed and thrill seeking, including the pursuit of a book and movie deal.

Force told the court:

> I'm sorry. I lost it and I don't understand a lot of it.

Bridges is due to be sentenced in December, and Force has been barred from communicating with his former colleague.

Police: Stop Posting Pictures of Your Kids on Social Media!

Police in Germany created a viral hit this week when they put out an urgent appeal for people to stop stripping children of their privacy.

The appeal, from police in Hagen, was posted, appropriately enough, on Facebook.

It was first posted on Tuesday, and by Friday morning, it had been shared by more than 245,000 people.

In the post, Hagen police noted that people freely post onto Facebook pictures of children nude while in a pool or at the beach, as if there were no consequences for posting such images.

From the translated post:

> Maybe you find the photos sweet today, but your child will find them endlessly embarrassing in a couple of years. Or your child will even be bullied. Even worse: a pedophile could use such photos for their purposes, publishing them elsewhere.

We already know that the average parent is like a loving but voracious paparazzo, uploading an eyeball-popping 973 photos of their child on social media by the time he or she reaches the age of 5, as online safety site The Parent Zone has reported.

We applaud Hagen police.

At Naked Security, we often point out, to all the oversharing parents out there, that posting photos of children is not necessarily safe behaviour - particularly when photo-posters are oblivious to privacy controls.

In fact, The Parent Zone study - done on behalf of safety campaign knowthenet - found that 17% of parents have never checked their Facebook privacy settings at all, while almost half (46%) have only checked once or twice, despite Facebook being the number one spot for sharing kid pics.

Look, we know that you very likely know how to set privacy controls on Facebook. We're preaching to the choir when it comes to readers of security blogs - many of you refuse to have Facebook accounts to begin with.

So do the kids in your life a favor: the next time you see images of some bare-bottomed tot being posted far and wide, don't just look away.

Don't tell the poster that the kid is adorable.

Instead, get stern.

Educate your peeps. Tell them what apps and sites their kids should steer clear of.

Definitely point them to our tips on how to make their Facebook account safer.

And by all means, please do point them to Facebook privacy controls.

Who knows? Maybe that little blue privacy dinosaur Facebook came out with last year can save kids from future harassment and abuse.

The 11 Worst Internet Scams We re Still Falling For

In 2001, I planned to move to a new town in Connecticut. I put my house up for sale, but it sat there, unsold in the recession, for over a year. Not a nibble, even after I dropped the price and made some improvements.

Then one day, my realtor called with some astonishing news. You ve got a full-price offer! she said. And get this: The buyer doesn t need an inspection, she s paying cash, and she wants to close at the end of this week!

OK, what? She didn t need a mortgage? She didn t want to negotiate?

Well, whatever. I showed up at the closing but the buyer herself was absent.

Her lawyer was deeply apologetic. She just called; she s in tears. She won t be buying your house after all. She just keeps saying, The Nigerian man promised that I d have the money by today!

Oh come on. Really? There s one person left in America who fell for the old Nigerian email scam?

No, not one person a lot of people. Internet scams are still a huge business. We sent Internet scammers $13 billion last year, and our gullibility shows no signs of abating.

All Internet scams are fundamentally the same: Someone offers you something you want for nothing. It s usually money, but it might also be male sexual prowess, weight loss, or a cure for baldness, herpes, cancer, cellulite, heart disease, diabetes, or deafness.

Here s a shocker: Not everything you read on the Internet is true. And so, for your own entertainment and education, here they are: The 11 hottest Internet scams that we re still falling for.

1. The Nigerian email scam

It comes to you by email:

I am Mr. Paul Agabi, it says. I am the personal attorney to

Mr. Harold Cooper, a national of your country, who used to work with Exxon Oil Company in Nigeria. On the 21st of April, my client, his wife and their only child were involved in a car accident. All occupants of the vehicle unfortunately lost their lives.

Amazingly enough, rich dead guy left behind millions of dollars and your correspondent wants you to have it! If you ll help Mr. Paul Agabi get those millions out of the country, using your bank account as a parking spot, he ll share the dough with you.

So you get excited. You write back. Maybe you make an offer on a house in Connecticut.

But then a funny thing happens: Mr. Agabi asks you to send some money to him, to cover bribes to officials. It s only a couple hundred bucks, so you send it.

A week later, there s another problem he needs another payment, this time to take care of taxes. You send it.

Then legal fees. Then other fees.

You will never get any money. You will be asked to send more, more, more money until you come to your senses and realize you re being bilked. Though it has expanded beyond the country of Nigeria, it is still called the Nigerian or 419? scam (named for the section of the Nigerian penal code it violates).

Yes, people still fall for the Nigerian scam. A lot of people. Commence mass forehead-slapping.

2. The perfect girlfriend scam

You re on a dating site, and you find The One: She s gorgeous, she s witty, and she s really into you. She really wants to meet you and she hints that your first date will be something you ll never forget. You re hooked, lined, and sunk.

Oh but she needs a little money for a ticket to come see you.

Oh, and can you help her out with her rent?

And how does it go when the big night arrives? It doesn t. She doesn t show up, because she s not a real person. She s a stock photo and a con artist who s been playing you probably a male.

3. The Craigslist scam

You re trying to sell something on Craigslist, the free classified-ads site a bicycle for $300, let s say. You hit paydirt almost immediately:

Send me your address, and I will mail you check right away for $1,500 to cover the bike and shipping to me in Germany. Deposit the check, and then send $450 by Western Union to my shipping company.

Maybe your spider-sense is tingling. But sure enough, you get a money order or certified check in the mail. Fantastic!

The only problem is, it s a forgery. You ll deposit it, wire this guy $450 of your real money and a couple of days later, your bank will let you know that the money order was a fake. Now you ve lost your bike and $450.

Three big clues that you re being targeted: (a) The offer is for more than you re asking; (b) you re supposed to send your item to another country; and (c?) you re asked to use the other guy s shipping company.

4. The classic phishing scam

You get an email from your bank (or Amazon, eBay, PayPal, Yahoo, Apple) saying that there s a problem with your account. You re encouraged to click the link to fix the problem or else your account will be suspended!

If you do click the link, though, you go a fake version of the bank s Web site. When you then log in, you re actually providing your name and password to the slimy Eastern European teenagers who are fishing for your login information, so they can steal your identity and make your life miserable. (This scam is called phishing because they re fishing for your information. And millions of people get scammed that way every year.)

If you have any concern that the message could be true, do not click the link in the email. Instead, open your Web browser and type in the company s address yourself (www.citibank.com or whatever). You ll discover, of course, that there s absolutely nothing wrong with your account.

Usually, though, you can tell at a glance that these emails are fake. They re filled with misspellings, typos, and the wording of a non-native English speaker. If it purports to be from Yahoo, it probably includes a graphic of the outdated logo:

Or here s a slick trick: If you point your cursor at the click here link without clicking, the pop-up bubble shows you what website will actually open, as you can see here. And guess what? It s not actually the bank/PayPal/Amazon!

5. The SMishing scam

Same thing as phishing, except that it arrives by text message (SMS) instead of email.

When you call the number to take care of the account problem, you get an automated voicemail system that prompts you for your account information.

6. The mugged on vacation scam

 Things got out of control on my trip to London, says an email from one of your friends. I was mugged, and all my belongings including cell phone and credit card were all stolen at gunpoint. I need your help flying back home and paying my hotel bills!

This one s especially confusing because the message comes from someone you know. (Sometimes, it s even purporting to be a family

member. It may even be a brief phone call instead of an email.)

Needless to say, your friend wasn t actually in London and hasn t been mugged.

Instead, the bad guys have planted software on your friend s computer that sent this same sob-story email to everyone in his address book. (In a variation on this, a scammer takes over your friend s Facebook profile and sends the message directly from there.)

If you re even a tiny bit persuaded that this note might be legitimate, Snopes.com (the Internet s clearinghouse for Internet rumors and scams) offers this superb advice:

Ask the caller a question that an impersonator would be unable to answer. Be careful to pose a question that requires more than knowledge of basic family information (e.g., names, birthdates, addresses), because that information is too easy for outsiders to look up instead, ask about something like a detail of a family event.

7. The pre-approved credit-card scam

Your current financial situation isn t so great right now, but hey, look at that it s your lucky day! You ve just gotten an email that offers a pre-approved Visa card! Or a loan with an impressively high credit limit. Hallelujah!

All you have to do is pay the annual fee up front.

Can you guess what happens next? Yes, you can: You never hear from them again. There never was a credit card or loan.

(Similar cons: You ve won a lottery! You ve landed a great job! You re invited to a great investment!)

8. The you ve-won-the-sweepstakes scam

Hey, wow! You just won an overseas sweepstakes one that you never even entered! How lucky can you be?

And get this once you supply your mailing address, you actually do get a check for a huge amount of money! They tell you to deposit it, but in the meantime, send them a check for a couple hundred bucks to cover processing fees and taxes.

Only one problem, which you can probably see coming down Sixth Avenue: Their check was bogus. Your check is real. The only one who made money from this sweepstakes is the scammer.

9. The work-at-home scam

At this point, you should be rolling your eyes. These Internet scams all follow a pattern.

The work-at-home scam is when you get an email offering you an amazing work-at-home job. Maybe it s stuffing envelopes, processing insurance claims, or processing credit-card transactions.

All you need to do is buy something up front: processing equipment, or a Web site, or access to a list of some type.

So you send the money, and guess what you get back?

Right. Nothing.

10. The false infection detected scam

You re on the Web, when a pop-up message appears, claiming that your computer might be infected by a virus. You re invited to click a link that will scan your system for infections. Surprise, surprise the scan discovers one!

And for the low, low price of $50, this mysterious remote company will clean up your PC for you.

If you fall for it, you ll spend the money and not get a cleanup
  in fact, you may wind up with a fresh installation of spyware.

11. The faux charity scam

Every time there s a disaster a hurricane, an earthquake millions of people, grateful to be safe and concerned for the victims, want to help.

And a few people want to cash in.

If, in the aftermath of a disaster, you get an email seeking money to help the victims, don t click. Instead, go directly to the Web site of a charity you know, and contribute there!
Human, meet Internet

None of this is new. None of this is surprising. The Internet may be the latest conduit for scams, hoaxes, and frauds but the greed, fear, and hope it exploits are as old as homo sapiens.

But here s the thing: homo sapiens means wise person. You have brains, too. Use them to steer clear of anything that s too good to be true.

Windows 10 Upgrade Become More Creepy, No Option to Opt-Out

If you are running Windows 7 or Windows 8.1 and have no plans to switch to Windows 10, then Microsoft could force you to install Windows 10, making it harder for you to cancel or opt-out of upgrading.

Reports are circulating that some Windows 7 and Windows 8.1 users are claiming that the latest Windows 10 OS has begun to automatically install itself on their PCs.

According to complaints by users, Windows Update screen is only offering them the option to either:

    Start the upgrade process, or

Reschedule the upgrade for a later date

Other users are finding that the dialog boxes they are presented display a message saying that the "Upgrade to Windows 10 is Ready," and prompting users to "Restart your PC to begin the installation."

The issue actually resided in the Windows Update process. Microsoft has listed Windows 10 as an "Optional" update, and normally these updates are unticked, meaning a user has to manually check them to install the OS it shouldn't be installed automatically.

However, Microsoft mistakenly checked these updates while listing them, which results in automatically installing Windows 10 on some computers running Windows 7 and Windows 8/8.1.

When reached out to Microsoft, the company said that the issue occurred with an optional update in Windows Update that was checked by default. Microsoft has now acknowledged the issue and reverted the checkbox, calling it "a mistake."

Mistake? Oh Really?

Here's the full official statement provided by Microsoft's spokesperson to Ars:

"As part of our effort to bring Windows 10 to existing genuine Windows 7 and Windows 8.1 customers, the Windows 10 upgrade may appear as an optional update in the Windows Update (WU) control panel. This is an intuitive and trusted place people go to find Recommended and Optional updates to Windows. In the recent Windows update, this option was checked as default; this was a mistake, and we are removing the check."

Just last month, Microsoft was caught downloading the Windows 10 installer files large gigabytes in size to Windows 7 and Windows 8 users, even without their knowledge.

Now this recent so-called mistake by Microsoft shows that how much the company is desperate to bring Windows 7 and Windows 8 users onto Windows 10, but there is a fine line between desperation and trust which the company has crossed many times.

Microsoft Will Release Threshold 2 Update for Windows 10 in November

While Microsoft announced Windows 10 as the final version of its flagship OS, subsequent updates were always part of the plan. The company was looking to construct a foundation which could be built upon for years to come, and now we have word that this process will start in November. Microsoft will release its Windows 10 Fall Update previously referred to internally as the Threshold 2 update next month, according to a report from Thurrott. The release has been given version number 1511 referring to the month and year of its release, which will apparently be the naming convention for future updates also. Users will receive this release as normal, via Windows Update. Along with a host of bug

fixes and other minor tweaks, it s also set to add some new functionality into Windows 10. Microsoft s new Edge browser is set to see some changes, too, although apparently not the often-requested addition of extensions.

Microsoft plans to launch payments service on Windows 10 soon An improved Media Creation Tool is set to be released via the update, and Cortana is set to gain some new abilities, including SMS text messaging to mobile phones directly from your PC. Meanwhile, a messaging app will introduce some features familiar to Skype users, according to reporting from Hexus. Additionally, extra customization options for the Start Menu are on their way, as well as some other UI improvements. We should see some icons swapped out for new versions, as well as changes to context menus and the option to recolor the title bars on Explorer windows. If you re currently running Windows 10, this update will be pushed to your computer as soon as Microsoft makes it available. Users that haven t yet taken the plunge will be able to move directly from previous versions of the OS to the Fall Update once it has been made available.

While Microsoft announced Windows 10 as the final version of its flagship OS, subsequent updates were always part of the plan. The company was looking to construct a foundation which could be built upon for years to come, and now we have word that this process will start in November.

Microsoft will release its Windows 10 Fall Update previously referred to internally as the Threshold 2 update next month, according to a report from Thurrott. The release has been given version number 1511 referring to the month and year of its release, which will apparently be the naming convention for future updates also.

Users will receive this release as normal, via Windows Update. Along with a host of bug fixes and other minor tweaks, it s also set to add some new functionality into Windows 10. Microsoft s new Edge browser is set to see some changes, too, although apparently not the often-requested addition of extensions.

An improved Media Creation Tool is set to be released via the update, and Cortana is set to gain some new abilities, including SMS text messaging to mobile phones directly from your PC. Meanwhile, a messaging app will introduce some features familiar to Skype users, according to reporting from Hexus.

Additionally, extra customization options for the Start Menu are on their way, as well as some other UI improvements. We should see some icons swapped out for new versions, as well as changes to context menus and the option to recolor the title bars on Explorer windows.

If you re currently running Windows 10, this update will be pushed to your computer as soon as Microsoft makes it available. Users that haven t yet taken the plunge will be able to move directly from previous versions of the OS to the Fall Update once it has been made available.

Google Rewarded The Guy Who Accidentally Bought Google.com, But He Donated It to Charity

Sanmay Ved the man who actually managed to buy Google.com got a huge reward from Google, but he donated all money to charity.

Last week, an ex-Google employee and now-Amazon employee managed to buy the world's most-visited domain Google.com via Google's own Domains service for only $12.

However, Ved owned Google.com for one whole minute before the Mountain View company realized it was a mistake and cancelled the transaction.

After acknowledging the mistake, Google rewarded Ved with some unknown amount of cash, but when Ved generously suggested donating his prize money to charity instead, Google just doubled the reward.

Ved believed that his real reward was just being the person who bought Google.com for a whole minute.

"I do not care about the money," Ved told in an interview with Business Insider. "It was never about the money. I also want to set an example that [there are] people who [wish] to find bugs that it's not always about the money."

Ved donated his reward to "The Art of Living India," an Indian foundation that focuses on providing education to poorer areas of the country.

Ved did not disclose the exact sum of cash Google had awarded him, but he did say that the amount was more than of $10,000.

That is a lot for just a few clicks!

Rare Apple 1 With Original First Manual Written by Apple Co-founder Ronald Wayne Up for Auction

Auction house Christie s currently has an Apple 1 computer up for auction with a starting bid of GBP 240,000 and an estimated sales range of GBP 300,000 500,000 [US$773,100].

Christie s description reads, in part:

The Apple-1 computer, born in 1976 of the computing genius of Steve Wozniak and the marketing drive of Steve Jobs, launched Apple Computer, a company that would define an industry and become the largest corporation in the world. What began as the attempt of two techie friends to design and build a microprocessor became the creation of the first personal computer, ultimately changing life around the globe. After introducing their new creation to a small group of like-minded friends at the Homebrew Computer Club in Palo Alto, California, Jobs and Wozniak were able to secure an order for 50 computers from Paul Terrell, owner of the Byte Shop, a small local retail outlet. The Apple-1 systems were sold without a

casing, power supply, keyboard or monitor, but offered a pre-assembled motherboard, something that put them far ahead of the competing self-assembly kits of the day.

THIS EXAMPLE COMES WITH THE EXTREMELY RARE FIRST MANUAL ISSUED BY THE APPLE COMPUTER COMPANY. Although not credited in the text, Ronald Wayne is well-known to be its author (and he does receive printed credit for drawing the enclosed schematics). The elder-statesmen of the Jobs-Wozniak-Wayne trio, Wayne drew the first Apple logo that appears on the cover of this pamphlet, drafted their partnership agreement, and wrote the present manual. His original logo symbolically connected the nascent Apple Computer Company to important scientific precedent: Sir Isaac Newton sits beneath an apple tree writing on several loose sheets, the glowing apple of inspiration above him, as if about to fall and spring forth innovation. Wayne also incorporated into his design Wordsworth s homage to Newton from The Prelude: A Mind forever voyaging through strange seas of thought alone. The backward-looking style of the logo, blending the Enlightenment s ideal of science and the Romantic s ideal of expression, could not conceal the overwhelmingly modern import of the simple text it announced.

Steve Wozniak, Steve Jobs, and the Apple INeither of the electrics nor electronics have been tested. We assume it could be brought up to working order again, as it was when last turned on in 2005, but we recommend a certified engineer attempt this. It is unknown if the capacitors are working but are seemingly sound. One chip at B12 incorrectly inserted. Scratches to motherboard by loose securing screw in bottom left not affecting circuitry. The reverse side has not been inspected since the motherboard is secured to the case with three firm screws. Some writing on motherboard in black ink C4   C14 and   74153 74 139 . Some parts possibly early replacements as is common with these machines that were initially bought by home enthusiasts. The manual [is] in very good condition noting the green title page appears to be an 1976 photocopy, as issued.

=~=~=~=

not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.